Board of Governors of the Federal Reserve System

AUDIT OF THE BOARD'S INFORMATION SECURITY PROGRAM

OFFICE OF INSPECTOR GENERAL

(A0205) ` September 2002

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

September 30, 2002

The Honorable Mark W. Olson
Chairman, Committee on Board Affairs
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Governor Olson:

We are pleased to present our *Report on the Audit of the Board's Information Security Program* (A0205). We performed this audit pursuant to the Government Information Security Reform Act (Security Act) which requires each agency Inspector General to conduct an annual independent evaluation of the agency's information security program and practices. This was the second year that such evaluations were required. Our specific audit objectives, based on the Security Act's requirements, were to evaluate the effectiveness of security controls and techniques for selected information systems and to evaluate compliance by the Board of Governors of the Federal Reserve System (Board) with the Security Act and related information security policies, procedures, standards, and guidelines. Appendix 1 to this report contains additional information on the Security Act and the Board's information security program; appendix 2 contains a more detailed description of our objectives, scope, and methodology.

To test security controls and techniques, we selected two applications for review. We performed our control tests using a modified version of the National Institute of Standards and Technology (NIST) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. Our tests did not identify any major security control weaknesses, although we found several areas where controls need to be strengthened. Given the sensitivity of the issues involved with these reviews, we are providing the results to management under separate restricted cover. We plan to follow up on implementation of our recommendations as part of our future audit activities related to the Board's implementation of the Security Act. We also followed up on the recommendations made during last year's control reviews and found that sufficient actions had been taken to close all recommendations on four of the five reviews; actions sufficient to close the fifth control review are in progress but have not been completed. We provided our follow-up letters to management under separate restricted cover and we will continue to track actions taken on the fifth review.

To evaluate the Board's compliance with the Security Act and related policies and procedures, we followed up on the seven recommendations in our 2001 Security Act audit report.[1] These recommendations were designed to help bring the Board into compliance with the

[1] *Report on the Audit of the Board's Information Security Program* (A0106), dated September 2001.

Security Act's requirements and further enhance the Board's information security program. Our follow-up work showed that actions had been initiated on most of the recommendations. Specifically, we found that the Board's Chief Information Officer (CIO) has taken steps to implement portions of the Security Act and that other components of the Board's organizational structure for information security have taken a broader perspective and more proactive approach to information security matters. We also found that management in the Division of Information Technology (IT) provided guidance to program officials to develop system specific security plans, defined major Board applications, established a mechanism to track major applications and associated reviews, reviewed application controls test plans, drafted guidance for defining a security incident program, developed an on-line security self-test for all Board staff, and reviewed risk assessments for all business functions

Notwithstanding the actions described above, issues remain open on portions of six of the seven recommendations. Specifically, we found that the roles and responsibilities of the CIO, program officials, the Information Security Officer (ISO), Information Security Unit, and the Information Security Committee have not yet been clearly defined (recommendations 1 and 2) and that several of the Security Act's key requirements have not yet been achieved as indicated by the open issues in our other recommendations. We believe it is essential that the responsibilities and authorities for these entities, particularly those of the CIO, be firmly established to ensure that the requirements of the Security Act are fully implemented and that the Board establishes a cohesive and consistent approach to information security. We believe this will help ensure that the relationships between these entities, as well as the responsibilities placed on them and the authorities they possess, are clearly understood by all staff. We also continue to be concerned that the ISO is not properly positioned within the Board's organizational structure to carry out his responsibilities effectively. In addition, our follow-up work showed that the CIO has not yet developed an agencywide information security plan (recommendation 3), established comprehensive corrective action plans for control review results (recommendation 4), finalized incident response guidelines (recommendation 5), or established specific information systems security training requirements (recommendation 6). Each of our original audit report recommendations and our analysis of the specific actions taken on each recommendation are discussed more fully in appendix 3 to this report.

The items still open from our prior audit relate to actions that must be taken to firmly establish the managerial responsibilities and guidance for the Board's information security program. These recommendations were designed to help establish the central, agencywide strategic authority that the Security Act envisions while emphasizing the security responsibilities inherent with all staff. Because all of the open items address requirements specifically cited in the Security Act, we believe that fully implementing the recommendations is essential for the Board to bring itself into compliance with the Security Act and to establish the organization and programmatic framework that the Security Act envisions. Implementing these recommendations will also assist management in establishing a centralized approach for issuing technical guidance and promoting staff awareness on information systems security best practices and procedures.

Because our independent evaluation did not identify any new recommendations, we have not requested written comments from Board management. Instead, we discussed the results of our work with the Staff Director for Management, who serves as the Board's CIO. The Staff

Director noted that the Board's management priority over the past year has been to implement the new plans stemming from the incidents of September 11, 2001, to enhance the resiliency of the Board's continuity of operations plans for key central bank functions including the critical IT systems that support the functions. Extensive IT resources have been redirected to enhance the Board's disaster recovery, physical security, and emergency voice and data communications infrastructures. The Staff Director believes that good progress on the Security Act has been made, particularly in light of the change in priorities. The Staff Director recognized, however, that further actions are needed to close out all of the recommendations regarding Security Act compliance. The Staff Director emphasized the need to continue to have a strong security culture throughout the Board and agreed to continue studying the issue of properly positioning the ISO within the organization. We will evaluate actions taken in response to the open portions of our previous recommendations as part of our continued work related to information security. Although the Security Act sunsets in 2002, legislation introduced in both houses of Congress would extend the Security Act's provisions or establish similar requirements going forward.

We are providing copies of this audit report to Board management officials and the report will be added to our publicly available web site. In addition, the Chairman will provide the report to the Director of the Office of Management and Budget as required by the Security Act. We will also summarize the report in our next semiannual report to the Congress. Please contact me if you would like to discuss the audit report or any related issues.

Sincerely,

Barry R. Snyder
Inspector General

cc: Governor Edward M. Gramlich
Governor Donald L. Kohn

APPENDIXES

BACKGROUND

Legislative Requirements

On October 30, 2000, the President signed into law the FY2001 Defense Authorization Act, including Title X, subtitle G, "Government Information Security Reform" (Security Act). The Security Act amends the Paperwork Reduction Act (PRA) of 1995 by enacting a new subchapter on "Information Security" and provides a comprehensive framework to ensure proper management and security of the information resources supporting federal operations and assets. The Security Act codifies existing information security requirements found in Office of Management and Budget (OMB) Circular A-130, Appendix III, and reiterates security responsibilities outlined in other legislation, including the Computer Security Act of 1987, PRA, and the Clinger-Cohen Act of 1996.[2]

The Security Act sets forth specific information security responsibilities for agency officials. The Security Act requires that each agency develop and implement an agencywide risk-based security program to provide information security throughout the life cycle of all systems supporting the agency's operations and assets. The Security Act emphasizes the CIO's strategic, agencywide security responsibilities, including responsibility for integrating the agency's security plan into the agency's performance plans and into the agency's enterprise architecture and capital planning and investment control processes.

The Security Act also places responsibility on agency officials for assessing the information security risks of the operations and assets for the programs and systems over which they have control. Officials are to determine, based on their risk assessments, the level of information security appropriate to protect such operations and assets and to periodically test and evaluate information security controls and techniques. The Security Act directs the program officials, in consultation with the CIO, to review each agencywide information security program at least annually.

The Security Act also establishes requirements for conducting annual independent evaluations of agency information security programs and practices. The independent evaluations are designed to test the effectiveness of security controls and techniques and to assess compliance with the Security Act's requirements. Responsibility for the independent evaluations has been given to the agency's Inspector General (IG). As required by the Security Act, each agency head is to submit the results of the IG's independent evaluation to the Director of OMB on an annual basis.

The Security Act gives the Director of OMB responsibility for establishing governmentwide policies for the management of information security programs. In July 2002, OMB issued memorandum 02-09 that provides updated guidance for agencies to implement the Security Act's requirements and report on the results of annual security reviews and independent evaluations. OMB's guidance focuses on three areas: agency progress in remediating security weaknesses

[2] The Legal Division of the Board previously determined that the Board is not subject to all provisions of OMB Circular A-130 or to the Clinger-Cohen Act of 1996. The Board is, however, subject to PRA and is therefore subject to the requirements contained in the Security Act.

identified last year; the results of current agency reviews and IG evaluations; and specific performance measures for agency officials accountable for information and information technology security. OMB's annual report to Congress, as required by the Security Act, will be based largely on the information agencies report according to these three areas. OMB's report will also measure progress against the performance baseline established in last year's security report to Congress.

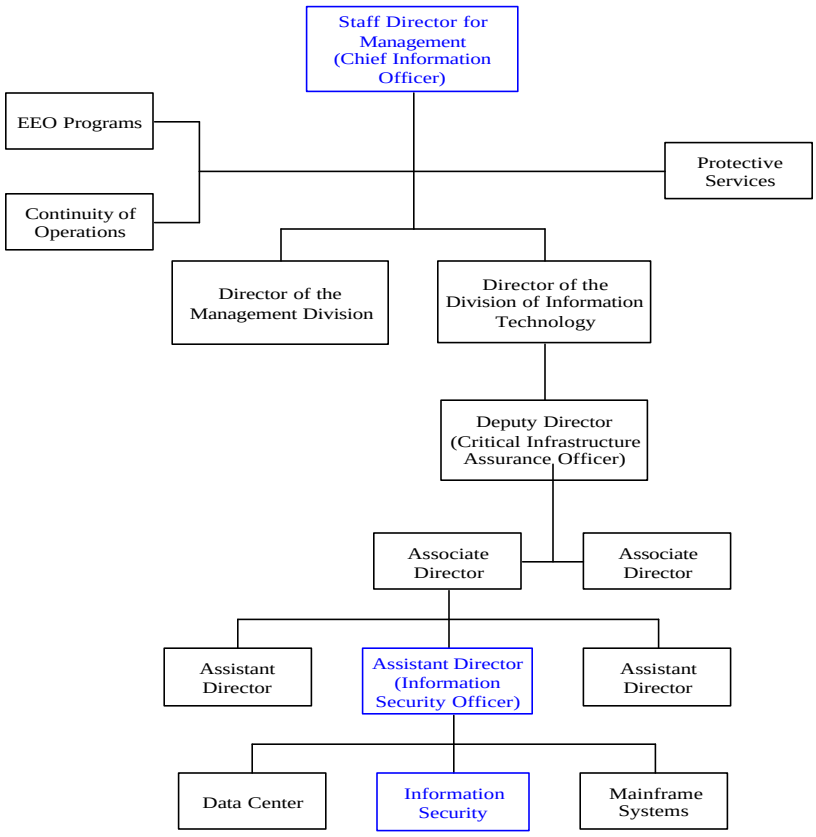
This is the second year that the IGs were required to conduct independent evaluations of their agency's information security programs and that agencies were required to submit the results to OMB. Although the Security Act is scheduled to sunset on October 30, 2002, there are two legislative efforts that could affect IG and agency responsibilities related to information security. The first is the Homeland Security Act of 2002, H.R. 5005, passed by the House in July, which contains language that would replace the Security Act in its entirety with essentially equivalent requirements. The second legislative effort is the E-Government Act of 2002, S. 803. This bill, which was passed by the Senate in June, would repeal the Security Act's sunset provision.

Information Security Roles and Responsibilities

The Board has designated the Staff Director for Management as the Board's Chief Information Officer. The Board's Information Security Unit, in the Division of Information Technology (IT), is responsible for monitoring the security of the Board's mainframe, public web sites, and local area networks. The unit is also responsible for intervening, as required, to address security exposures and for acting as liaison to Federal Reserve System (System) groups coordinating Systemwide security issues. The Information Security Unit reports to an IT assistant director who serves as the Board's ISO and is the focal point for the Board's information security activities. (See the organizational chart that follows.)

Appendix 1

Board Organizational Chart for IT and Information Security



Because much of the information technology at the Board is decentralized, divisions and offices also have information security responsibilities. Specifically, network administrators are responsible for configuring, maintaining, and protecting the systems under their control to ensure a secure distributed operating environment. Information owners are responsible for assessing the degree of business risk associated with their systems and applications, classifying and authorizing access to information, and ensuring proper security controls are in place. To help coordinate these responsibilities, the Board has established an Information Security Committee (ISC) comprised of representatives from each division and office. The ISC functions as a Boardwide coordinating body with responsibility for advising management regarding System information security strategic direction and initiatives. The ISC is also responsible for the local application of policies and procedures in support of System information security policies and safeguards.

Information Security Guidance

To provide policy direction regarding the protection of its information assets, the System developed the *Information Security Manual* (ISM). The ISM defines policies and safeguards for information security and is applicable to all automated platforms and manual information processes used throughout the System. The ISM is built on three security principles: confidentiality (assurance that information is disclosed only to authorized entities), integrity (assurance that information has not been improperly altered), and continuity of operations (assurance that correct information is available when needed). Two other manuals, the *Distributed Processing Security Support Manual* and the *Mainframe and FEDNET Security Support Manual*, contain policies and procedures specifically related to those information technology environments and support the general guidance provided by the ISM.[3] Board divisions and offices are required to comply with the policies and safeguards in these manuals.

Information Technology Architecture

The Board's information technology architecture includes mainframe and distributed operating environments. The Board relies heavily on its mainframe computer system to process and analyze data used in making monetary and economic policy decisions and in performing its other regulatory, operational, and administrative activities. Many of the Board's mission-critical systems are mainframe applications, underscoring the need to provide a secure and reliable mainframe processing environment. Mainframe operations are IT's responsibility, although Board divisions and offices are considered the data owners.

While mainframe computer operations are used for large-scale processing and storage, the Board has shifted resources to provide analytical tools to users at their desktops. Desktop computing operations give users powerful, cost-effective tools for convenient access and greater control over data. In a distributed environment, however, operational management functions such as security, backup and recovery, and problem resolution may not be as fully developed as for mainframe operations. To address this potential control weakness in the distributed processing environment, the Board relies on the development of effective processes for detecting and controlling distributed processing activities and on establishing appropriate backup and disaster recovery procedures. The Board's distributed processing environment includes Microsoft Windows and UNIX-based servers, personal computers, laptops, and the associated telecommunications infrastructure. IT is generally responsible for distributed hardware, software, and communications, although some divisions and offices maintain their own

[3] The *Distributed Processing Security Support Manual* contains safeguards specific to distributed processing environments, such as personal computers, external network connectivity, local area networks, wide area networks, and telephonic systems. The *Mainframe and FEDNET Security Support Manual* contains safeguards specific to mainframe computers and FEDNET Communications equipment.

processing platforms. In a distributed processing environment, Board divisions and offices are still considered the data owners and may also have responsibility as the data custodians.

OBJECTIVES, SCOPE AND METHODOLOGY

We conducted our audit fieldwork from April to September 2002. Our audit objectives, based on the Security Act's requirements for conducting independent evaluations, were to evaluate the effectiveness of security controls and techniques for selected information systems and to evaluate the Board's compliance with the Security Act and related information security policies, procedures, standards, and guidelines.

To achieve our objectives, we reviewed Board and System documentation pertaining to information security and met with officers and staff throughout the Board with information security responsibilities. To test security controls and techniques, we selected two applications for review and evaluation. The following table shows the platform and division or office for each application included in our review. We performed our control tests using a modified version of the NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. NIST Special Publication 800-26 provides specific control objectives and techniques related to management, operational, and technical information system controls. We also followed up on the status of recommendations made for the five security control reviews we completed during 2001.

Applications Included in Office of Inspector General (OIG) Control Testing

APPLICATION[4]	PLATFORM	DIVISION/OFFICE
Federal Reserve Integrated Records Management Architecture (FIRMA) System	Unix-based Distributed	Office of the Secretary
Reporting Panel Management System (RPMS)	Mainframe	Research and Statistics

To evaluate the Board's compliance with the Security Act, we followed up on the status of the recommendations made in our 2001 independent evaluation of the Board's information security program and practices.[5] We also reviewed the methodologies developed by Board staff and independent Board consultants for performing system control reviews. Finally, we compiled information on those areas for which OMB requested a specific response as part of the agency's annual Security Act reporting. Our audit was conducted in accordance with generally accepted government auditing standards.

[4] The FIRMA system, in conjunction with manual operations, converts the Board's paper records into electronic records and manages them in compliance with federal records management laws and regulations. RPMS represents a set of DB2 tables that contain current and historical information about each of the Board's reporting series.

[5] See our *Report of the Audit of the Board's Information Security Program* (A0106), dated September 2001.

ANALYSIS OF ACTIONS TAKEN ON PRIOR RECOMMENDATIONS

Original Recommendation #1

We recommend that the Administrative Governor clearly define the roles and responsibilities of the CIO and program officials to encompass all requirements contained in the Security Act.

Basis for the Original Recommendation

The Security Act outlines a number of significant security-related responsibilities for individuals within each agency. For example, the Security Act defines the CIO as having responsibility for providing a strategic view of the agency's architecture and crosscutting security needs. The Security Act directs agency CIOs to develop, implement, and maintain an agencywide security program, describe the program in detail in an agencywide security plan, and ensure that the program is fully integrated into the agency's enterprise architecture and capital planning and investment control processes. The CIO is to work with agency program officials, who are responsible for developing, implementing, and maintaining a security program (and documenting it in a security plan) that assesses the risk of, and provides adequate security for, the operations and assets of programs and systems under their control. Agency program officials should also periodically test and evaluate information security controls and techniques for their programs and systems.

Last year, we found that although the Administrative Governor had designated the Staff Director for Management as the Board's CIO, the designation memorandum did not delineate any specific responsibilities or set any expectations. We also found that while the ISM assigned program officials the responsibility for performing some of the functions enumerated in the Security Act, the ISM did not include other functions such as developing system-specific security plans. The manual also did not specify the frequency, scope, or reporting requirements for conducting periodic security controls reviews.

Actions Taken

At a senior management meeting earlier this year, the Administrative Governor had the CIO and the Chief Infrastructure Assurance Officer (CIAO) explain the roles and responsibilities of the CIO and program officials to all of the division directors. Per the CIAO, the discussion encompassed all requirements contained in the Security Act.

Analysis of Actions Taken

Although the Staff Director for Management has been delegated the CIO function for the Board and has taken steps to implement the Security Act's requirements, key elements of the Security Act remain unfulfilled. The CIO has not, for example, developed a Boardwide security plan, provided guidance for developing corrective action plans, finalized incident response procedures, or established security-related training requirements. We continue to believe that clearly defining the CIO's specific information systems security roles and responsibilities is important given the significant, agencywide responsibilities the Security Act establishes for this position. Clearly establishing the expectations for program officials will, likewise, help ensure that they continue to fulfill their responsibilities under the Security Act. It will also provide for a stronger, more cohesive information systems security program at the Board by emphasizing that information systems security, like financial management or human capital management, is the responsibility of each division director. Beyond a verbal explanation, however, we believe that establishing the expectations for the CIO and program officials in a single document (such as the Boardwide information security plan discussed under recommendation 3) would help ensure that the requirements and the interrelationships are clearly understood by all concerned.

Documenting roles and responsibilities in a security plan would also enable the Board to clarify the various security-related responsibilities of other senior officials. For example, the Administrative Governor has delegated responsibility for information security to the Staff Director for Management who has, in turn, delegated responsibility to the Director of IT. The delegations do not, however, distinguish between the CIO's strategic, policy-related responsibilities and the Director of IT's operational responsibilities as related to information systems security. We also believe the Administrative Governor or the CIO should clarify the role of the CIAO (who is also the Deputy Director of IT), especially since the CIAO has taken a leading role in implementing many of the Security Act's requirements.

Status of the Recommendation

Open.

Original Recommendation #2

We recommend that the CIO (a) clarify the roles and responsibilities of the ISO, the Information Security Unit, and the ISC in light of the Security Act's requirements, and (b) reevaluate the ISO's organizational placement.

Basis for the Original Recommendation

The Security Act directs the CIO to designate a senior agency information security official who reports to the CIO or a comparable individual within the agency. This official's responsibilities should include reporting to the CIO on the implementation and maintenance of the agency's information security program and policies. Last year we concluded that the ISO, along with the Information Security Unit and the ISC, formed the basic organizational framework at the Board to assist the CIO in fulfilling the Security Act's requirements. We recommended that the CIO more clearly define the roles and responsibilities of each of these entities to provide them with the necessary strategic perspective and operational direction. We noted that the ISO in particular will likely become the focal point in many instances for implementing the Security Act's requirements, and that fulfilling this responsibility would, in our opinion, require the ISO to possess a strategic, agencywide perspective with specific cross-cutting responsibilities and strong senior management support. Along this line, we expressed concern that the ISO was four organizational levels removed from the CIO and that the ISO had other significant information technology related responsibilities.

Actions Taken

The ISO and the Information Security Unit have taken a more proactive role in providing guidance to divisions on information systems security matters, such as providing guidance for control reviews and risk assessments. During 2002, the Information Security Unit conducted systems security control reviews for five of the Board's major applications. The ISC, which is chaired by the ISO, met more frequently during 2002 and has taken on greater Boardwide information systems security responsibilities. In addition, the CIO indicated that he reviewed the ISO's organizational placement but concluded that no changes were required.

Analysis of Actions Taken

We continue to believe that the roles and responsibilities of the ISO, the Information Security Unit, and the ISC need to be clarified in light of the Security Act's requirements. Although these entities have assumed a broader perspective and adopted a more proactive approach, the specific expectations need to be clearly established to ensure that all aspects of the Security Act, or the successor legislation, are fully implemented as part of the Board's security program. We believe that defining the responsibilities and authorities for the ISO is particularly important in order to invest this position with the Boardwide authority needed for providing guidance and direction

and for ensuring that the Security Act's requirements are implemented in accordance with established guidelines.

Although the ISM provides basic guidance, we believe that a Boardwide security plan would provide a better vehicle for enumerating all security-related requirements, including those unique to the Board. Outlining the expectations in a Boardwide plan would clearly establish the relationships between these entities and the CIO and program officials. This would also help ensure that all Board staff understand the expectations that have been placed on the ISO, the Information Security Unit, and the ISC, as well as reinforce their authority for providing information systems security guidance across the Board.

We also remain concerned that the ISO is not properly positioned within the Board's organizational structure to effectively carry out his information systems security responsibilities. The ISO has ongoing day-to-day operational information technology responsibilities, including the responsibility for the Board's data center and for support of the Board's mainframe operations. These operational responsibilities could create a conflict of interest with performing other information security activities as required under the Security Act. We believe that separating the information security function into an independent entity headed by the ISO with a line of reporting to the CIO, rather than to operational information technology management, would enhance the ISO's ability to focus on security issues as well as ensure a more direct route to senior management on matters that have Boardwide implications.

Status of the Recommendation

Open.

Original Recommendation #3

We recommend that the CIO develop an agencywide information security plan and establish guidance for program officials to develop system-specific security plans.

Basis for the Original Recommendation

The Security Act and subsequent guidance outlined that agency CIOs were to develop, implement, and maintain an agencywide security program that assessed risk and provided adequate security for the operations and assets of all agency programs and systems. The information security program was to be documented in an agencywide security plan. In addition, the guidance required program officials to develop a security plan for each system under their control. Last year, we found that although the ISM contained some of the elements of a security plan, and that additional elements of system-specific plans existed in other documents (such as user manuals, risk assessments, and continuity of operations plans), the Board's CIO had not developed an agencywide information security plan nor had the CIO required each program official to develop plans tailored to the systems or applications under his or her control.

Action Taken

IT management provided guidance to all divisions and offices for developing system-specific security plans; the guidance included a template covering the areas outlined for security plans in OMB Circular A-130. IT management also directed divisions and offices to focus on developing security plans for those systems designated as major applications. As of early September 2002, security plans for all of the Board's major applications had been completed or were expected to be completed by November 2002. IT management is also developing an approach for completing plans for the remaining non-major systems. In addition, IT management developed a list of remedial actions that have been taken or need to be taken to address the concerns raised in our 2001 Security Act audit; this one-page document has been designated as the Boardwide security plan.

Analysis of Actions Taken

The guidance provided for developing system-specific security plans is sufficient to close the latter part of the recommendation. There has been limited progress, however, towards developing an agencywide information security plan. We continue to believe the CIO should develop a separate Boardwide security plan using the ISM as a frame of reference. Rather than simply restate the ISM, however, the plan should reflect the Board's information technology architecture, its organizational structure, and those requirements unique to the Board (such as compliance with federal laws and regulations) that are not found in other System entities. Whether the CIO elects to develop a formal Board policy or a set of guiding principles, we believe that the document should serve as a Board-specific security blueprint that addresses the vision and the underlying philosophy for information security at the Board. This document

would also serve as a mechanism for documenting the security-related roles and responsibilities as discussed in recommendations 1 and 2, as well as some of the other Security Act related issues discussed in our other recommendations.

Status of the Recommendation

Partially closed.

Original Recommendation #4

We recommend that the CIO enhance the security control reviews by (a) clearly defining major Board applications, (b) establishing a mechanism to track applications and associated reviews, (c) reviewing test plans and results, and (d) providing guidance for establishing corrective action plans.

Basis for the Original Recommendation

The Security Act requires that agency officials periodically test and evaluate the information security controls and techniques for the systems under their control. As we noted last year, conducting periodic system reviews was not a new requirement for most federal agencies since OMB Circular A-130, Appendix III, already required periodic reviews of security controls for an agency's general support systems and major applications.[6] We found, however, that the Board had not conducted the types of reviews described in the circular. Although the ISM required management to conduct periodic security reviews that focused on the adequacy of, and compliance with, information security policies, these reviews had generally not been conducted or were limited to an application's development phase.

Actions Taken

IT management provided divisions and offices with additional guidance to define major applications based on the requirements found in OMB Circular A-130. Working with the divisions and offices, IT management subsequently identified twenty-five major Board applications and three general support systems. IT also established a web page to track the status of the security plans and the control reviews for the major applications and general support systems. Based on subsequent OMB guidance, IT developed a complete list of all Board applications; 178 systems have now been identified Boardwide. Since our 2001 audit, the Board has continued to conduct control reviews, both internally and through the use of an independent consulting firm. Board staff developed test plans for those systems to be tested internally and IT management reviewed the consultant's plans prior to authorizing the reviews.

Analysis of Actions Taken

The actions described above are sufficient to close the first three parts of our recommendation. We note, however, that IT should update its tracking web page to monitor the development of security plans and the completion of control reviews for the remaining Board systems. We

[6] General support systems are defined in the circular as an interconnected set of information resources under the same direct management control and which share common functionality. General support systems could include a local area network, a communications network, or a data processing center. A major application is defined as an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

believe this will help bring the Board in line with recent OMB guidance concerning annual reviews of all agency systems.

Because the CIO has not yet provided guidance for establishing corrective action plans, this portion of our recommendation remains open. As reviews are completed and weaknesses identified, the CIO should ensure the weaknesses, associated corrective actions, and assigned responsibilities are documented in a plan of actions and milestones (POA&M) as described in OMB guidance. The POA&M is designed to serve as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps. The POA&M should also include any deficiencies identified through other information systems reviews, such as the recent test by the System's Virtual Competency Center. In keeping with OMB's July 2002 guidance, we plan to review the Board's POA&M before it is submitted to OMB later this year.

Status of the Recommendation

Partially closed.

Original Recommendation #5

We recommend that the CIO develop guidance that more clearly defines a "security incident" and establish Boardwide procedures for incident reporting.

Basis for the Original Recommendation

The Security Act reiterated existing guidance that all agency security programs should include procedures for detecting, reporting, and responding to security incidents. The intent of the Security Act's security incident provision was to ensure that each agency had both the technical and procedural means in place to detect and appropriately report security incidents and share information on common vulnerabilities. All agency security programs were to include policies and procedures that removed unnecessary internal obstacles for timely reporting of security incidents to the appropriate agency authorities, as well as to law enforcement authorities and other external organizations.

During 2001, the System established a National Incident Response Team (NIRT) to play a leading role in System efforts to protect information systems and data resources against unauthorized use and from external attacks. The Federal Reserve Bank of New York (FRB NY) headed the response team and was responsible for establishing Systemwide response procedures. FRB NY was also responsible for determining what, if any, external reporting of security incidents is appropriate. Because the System's response team was still in the formulation stages, specific guidance and response procedures had not yet been developed. The Information Security Unit had prepared incident reporting procedures for Board operations. However, the procedures only applied to automation resources managed by IT. The procedures did not address the responsibilities of other divisions and offices for identifying or reporting a security incident nor did the procedures discuss external reporting requirements. We found that the ISM also provided some additional guidance, but the guidance did not clearly define what constitutes a security violation or establish complete reporting requirements.

Actions Taken

The ISO recently provided the ISC members with draft incident response procedures for review. The draft procedures outline the steps for Board staff and management to follow to ensure an efficient and effective response in the event of a possible or actual security incident. The procedures also address incident reporting and escalation processes within the Board as well as to external parties such as NIRT, the Federal Computer Incident Response Center (FedCIRC), and the National Infrastructure Protection Center (NIPC).

Analysis of Actions Taken

The draft procedures, if effectively distributed and implemented, will satisfy the intent of our recommendation. As we noted in last year's audit report, the guidance must be communicated to all Board staff and must clearly define what constitutes a security incident. The ISO has discussed, and we endorse, using the Board's intranet to disseminate the new guidance. The ISC could also be used as a supplemental delivery mechanism. When the guidance is disseminated, we encourage the ISO to ensure that the term "security incident" is clearly defined using examples that staff might encounter during normal business activities. In addition, the ISO should clarify the relationship between the Board and NIRT for reporting security incidents. During our audit, the Board's liaison to NIRT expressed difficulty in interacting with FRB NY staff, and in our discussions with NIRT officials, they indicated concern regarding Board participation in this System function.

Status of the Recommendation

Open.

Original Recommendation #6

We recommend that the CIO enhance the Board's security awareness and training program by (a) requiring all staff to complete an annual security refresher course, (b) establishing additional proactive measures to promote security awareness, (c) establishing specific training requirements for all staff with information security responsibilities, and (d) developing a tracking mechanism to ensure that information security training requirements are met.

Basis for the Original Recommendation

The Security Act requires the agency CIO to ensure the agency has personnel sufficiently trained in their security responsibilities to assist the agency in complying with the requirements of the Security Act and related policies, procedures, standards, and guidance. The Security Act also requires agency security programs to include security awareness training to inform personnel of relevant information security risks and their responsibilities to reduce such risks. These requirements reiterate those of the Computer Security Act of 1987, which specifically requires each agency to provide mandatory periodic training in computer security awareness and accepted computer security practice to all employees involved with the management, use, or operation of a federal computer system. The General Accounting Office noted in its *Federal Information System Controls Audit Manual* that the leading organizations they studied considered security awareness to be one of the most important factors in the overall risk management process.

Last year we found that the Board had developed a security awareness program consisting of training new employees during initial employee orientation and posting periodic articles on "Inside the Board" related to computer viruses and other information security issues. The Board had not, however, developed annual refresher training for Board staff, considered other methods to promote security awareness, or developed a security training program for those individuals with specific information security responsibilities.

Actions Taken

IT recently developed an on-line security self-test for all staff with access to the Board's network. Since our 2001 audit report was issued, IT has posted additional articles on "Inside the Board" to provide additional security awareness training related to passwords, secure e-mails, and social engineering. IT management also requested that each division and office identify staff with significant security responsibilities and, for each staff member identified, list the types of information security and technical classes, conferences, and seminars taken during 2001 and 2002.

Analysis of Actions Taken

Although the on-line security self-test meets the intent of an annual refresher course and is sufficient to close this part of the recommendation, we believe that IT should consider ways to enhance the process going forward. Rather than simply reference the ISM and "Inside the Board" articles, the self-test could first present the security-related information that IT management wants to emphasize and then ask questions specifically related to this information. We note that at least one Reserve Bank has developed an on-line security awareness program that guides staff through security awareness information, ending with a short self-test to reinforce the materials presented.

We continue to believe that other options exist to promote security awareness and this portion of the recommendation remains open. We have suggested to IT management that the Board's intranet home page include a link to an information security web page that contains the "Inside the Board" articles, the refresher self-test, and other security-related information. The page should be routinely updated with new information security topics to help make security awareness more of an ongoing/continuous process. The additional updates could encompass information and tips that other agencies have typically placed on posters and various giveaways to sustain employee interest in security awareness. Another proactive measure that we recommended in 2001 and continue to endorse is requiring each employee to acknowledge, in writing, that they have read and that they understand the Board's information security requirements and that they are aware of the penalties for failing to comply. New employees are provided with an "Annual Information Security Statement" during orientation; however, long time employees at the Board may be unaware of its existence and requirements. This could also be incorporated into the on-line self-test.

By identifying staff with significant security responsibilities and the types of training these individuals have received, IT has taken sufficient action to close the final part of this recommendation. The CIO should now, however, use this information to develop specific training requirements. Establishing a training benchmark will help promote consistency to ensure the Board maintains a high-quality, security-conscious technology staff. The requirements could be in the form of recommended classes or the CIO could use the Board's training infrastructure to provide in-house information security training.

Status of the Recommendation

Partially closed.

Original Recommendation #7

We recommend that the CIO enhance the Board's risk assessment program by ensuring that periodic risk assessments are conducted in compliance with ISM requirements.

Basis for the Original Recommendation

Last year, the CIO issued guidance to all Board divisions and offices requiring that risk assessments for each business functional area be updated and that each division director provide a report to the CIO stating that risk assessments were current. The guidance was in keeping with the ISM requirement that risk assessments be performed for all business functions and that the assessments be periodically updated and revised, as needed, for any operational changes. We recommended that the risk assessments be submitted for review by the CIO or ISO to promote consistency, identify common vulnerabilities, and provide additional guidance as required.

Actions Taken

IT management directed each division and office to complete a risk assessment for their business functions and submit the completed assessments to the ISO. The ISO also established an ISC subcommittee to review the completed assessments.

Analysis of Actions Taken

Although the actions taken are sufficient to close the original recommendation, we note that the subcommittee's review concluded that the divisions and offices did not follow the same methodology and that the assessments did not provide consistent information. Our review of the completed assessments showed that the information provided to the ISO varied in format and content. The ISO has recognized that additional guidance beyond the ISM is required to eliminate the wide variation and to ensure that divisions and offices use the same methodology in developing their risk assessments. The ISO also plans to establish a requirement for annual updates, or at least require divisions and offices to submit a statement that nothing has changed.

In closing this recommendation, we also note that when the guidance is revised and the new risk assessments are submitted, the ISO should review the results to identify any vulnerabilities and provide specific guidance as required for implementing corrective actions. Any issues identified through the risk assessment review process should also be tracked on the Board's POA&M to help provide a complete picture of the Board's information systems security status. In addition, we note that the ISM risk assessment approach requires the assessment to be performed from a division's business function risk approach rather than focusing specifically on the risks that may be present for an applicable system within the division or office. The ISO may want to consider

shifting the risk assessment process from a business function perspective to a system focus to facilitate identifying the risks and required mitigating controls for specific systems.

Status of Recommendation

Closed.

Appendix 4 – Principal Contributors to this Report

William Mitchell, Program Manager

Robert McMillon, EDP Auditor and Auditor in Charge

Ronald Braciak, EDP Auditor

Ariane Ford, Auditor

Paul Sciannella, EDP Auditor